****
IT SERVICE MANAGEMENT NEWS
****

Newsletter mensile con novità in materia di sicurezza delle informazioni, IT Service Management, Qualità.
E' possibile dare il proprio contributo e diffonderla a chiunque secondo la licenza
http://creativecommons.org/licenses/by-nc/2.5/it/

E' possibile iscriversi o disiscriversi
- scrivendo a cesaregallotti@cesaregallotti.it
- seguendo le istruzioni riportate nella pagina http://www.cesaregallotti.it/newsletter.htm.
Sulla stessa pagina è possibile consultare l'informativa sul trattamento dei dati personali.

****
Indice

****
01- Videosorveglianza

Come se fosse una risposta alla sentenza della Cassazione segnalata il mese scorso (http://ziczac.it/a/leggi/014261a250704ef37ab70a3f19538f82/), il Garante della Privacy emette un Provvedimento di blocco delle videoriprese via webcam all'interno di due negozi a scopo di sicurezza perché non sono rispettate le norme dello Statuto dei lavoratori che vietano il controllo a distanza dei dipendenti.
http://www.garanteprivacy.it/garante/doc.jsp?ID=1736167

Proseguo la mia polemica con l'Ufficio del Garante: la notizia si trova sulla Newsletter del Garante del 19 luglio 2010, senza riferimenti puntuali o link al Provvedimento.

****
02- Certificazioni professionali

Dalla newsletter SANS NewsBites Vol. 12 Num. 58 si trova la notizia che negli USA c'è carenza di capaci professionisti della sicurezza (per il monitoraggio e la gestione degli attacchi, per lo sviluppo, per la programmazione sicura, eccetera).

Da qui, il Center for Strategic and International Studies (CSIS) ha commentato che "l'attuale sistema di certificazioni professionali non è solo inadeguato; sta creando un falso senso di sicurezza" perché sono più orientate a sviluppare le capacità di redazione di documenti conformi a qualche normativa o regolamento e non a sviluppare capacità di riduzione dei rischi.

Purtroppo il proliferare di certificazioni professionali (lo si dice da tempo) è negativo per i "clienti" che si fidano troppo ciecamente di un attestato e per i professionisti che devono spendere un mucchio di soldi e tempo per avere una serie di diversi fogli di carta che attestano competenze similari.

http://www.informationweek.com/news/smb/security/showArticle.jhtml?articleID=226100078
http://www.abc.net.au/news/stories/2010/07/22/2961755.htm?section=world
http://www.npr.org/templates/story/story.php?storyId=128574055
http://csis.org/publication/prepublication-a-human-capital-crisis-in-cybersecurity

****

03- SAS 70

Dalla newsletter ISACA@AGlance del luglio 2010 si ha la notizia della futura suddivisione dello standard SAS 70 in due parti, dedicate rispettivamente ai report emessi dal fornitore di servizi e dall'utilizzatore dei servizi.

https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/New-Service-Auditor-Standard-A-User-Entity-Perspective.aspx

****

04- Statistiche sugli attacchi IT

Sulla newsletter SANS NewsBites Vol. 12 Num. 60 è stata segnalata la pubblicazione del Verizon's Data Breach Investigation Report.

La "notizia" è che il 70% degli attacchi rilevati sono di origine esterna.

Forse questo lo sapevamo già, ma il report è comunque interessante.

Un breve riassunto: http://isc.sans.edu/diary.html?storyid=9283
Il report: http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

****

05- Threatsaurus

Franco Ferrari del DNV Italia mi segnala il "Threatsaurus - Minacce informatiche e sicurezza dei dati dalla A alla Z" della Sophos.

Opuscolo semplice ma non banale sulle minacce IT:
http://www.sophos.it/sophos/docs/itl/papers/sophos-threatsaurus-a-z-it.pdf

****

06- Cloud computing

Segnalo il bell'articolo di Marco Mattiucci sul Cloud Computing, che tratta di aspetti funzionali e di Digital Forensics
http://www.marcomattiucci.it/cloud.php

****

07- Come gestire gli auditor

Simone Tomirotti dell'AIEA (che ringrazio) ci segnala l'articolo "1 in 10 IT professionals admit to cheating to get an IT audit passed": http://bit.ly/bDo1EH

Simone Tomirotti dice anche "Mi ha colpito che la balla (o scusa) principale che viene usata è la mancanza di risorse e di tempo, per sottolineare la pressione subita".

Aggiungo che un mio amico (italiano) quando ha segnalato le sue difficoltà su risorse e tempo ad un collega (inglese), quest'ultimo gli ha risposto laconicamente "Poor planning" (tradotto ed

esplicitato: "TU hai pianificato male").

Le tecniche di gestione di un auditor sono tante, alcune efficaci ("siamo molto contenti di avere il suo audit, così ci potrà sengalare utili aree di miglioramento"), altre meno (il pranzo lungo). Il "commuoverlo" è buona.

****

08- Dare in outsourcing l'application management: qualche rischio

In seguito alla segnalazione del mese scorso in merito ai rischi di sviluppatori non eticamente corretti, Andrea Rui mi ha segnalato la sua conoscenza "di un programmatore COBOL che qua e là inseriva nel codice dei cicli di for, per rallentare l'esecuzione del codice;
poi veniva chiamato per l'ottimizzazione del codice ..."

Grazie per la segnalazione.

****

09- Tipologie di standard (Errata corrige)

Tony Coletta mi ha segnalato un errore nella newsletter di luglio, dove si indicavano le differenze tra International Standard, Technical Standard, Technical Report, Publicly Available Specification

Riporto quindi di seguito un riassunto dello scambio di email (spero di non aver fatto errori)

COLETTA: I quattro tipi di documento sono tali perchè diversi in natura, non perché approvati con diversi livelli di consenso.

Delle direttive ISO (tra cui la ISO/IEC Guide 2:2004) definiscono i vari tipi di documento, i loro diversi scopi ed i diversi livelli di consenso necessari per la loro approvazione:
- IS : document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context
- Technical Specification (TS): document published by ISO or IEC for which there is the future possibility of agreement on an International Standard, but for which at present the required support for approval as an International Standard cannot be obtained, there is doubt on whether consensus has been achieved, the subject matter is still under technical development, or there is another reason precluding immediate publication as an International Standard
- Technical Report (TR): document published by ISO or IEC containing collected data of a different kind from that normally published as an International Standard or Technical Specification
- Guide: document published by ISO or IEC giving rules, orientation, advice or recommendations relating to international standardization
- Publicly Available Specification (PAS): document published by ISO or IEC to respond to an urgent market need, representing either a consensus in an organization external to ISO or IEC, or a consensus of the experts within a working group

GALLOTTI: "Mi viene comunque da pensare che la tipologia di documento (IS, TR, TS, PAS) venga decisa sulla base della previsione di livello di consenso"

COLETTA: E' vero che la tipologia di documento è decisa preventivamente, ma non sulla base di una previsione di percentuale di voti favorevoli che si pensa di ottenere.

Per esempio quando abbiamo avviato i lavori di SPICE (ISO/IEC 15504) abbiamo deciso che la prima emissione sarebbe stata sotto forma di TR di tipo 2, perché pensavamo che l'approccio proposto poteva non essere abbastanza maturo e quindi richiedeva un periodo esteso di trial sul campo prima di decidere se promuoverlo a IS.

I TS infatti, possono esistere per un massimo di 3 anni. Dopo di che bisogna riesaminare la situazione e decidere se ritirarli o tentare di farli approvare come IS, magari previa revisione.

E' proprio quello che abbiamo fatto con la 15504.

GALLOTTI: Vorrei avere conferma di questo fatto: la tipologia di documento non esclude il loro uso a scopo di audit anche di certificazione; per esempio ho in mente la ISO TS 16949 per la qualità in ambito automotive, sulla quale sono condotti audit e rilasciati certificati di conformità.

COLETTA: Per quanto riguarda la "certificabilità", i TR e i TS e possono essere oggetto di verifica di conformità purché contengano requisiti (shall statement).